System Administrator=s Manual (SAM)
COURTNEY Version 1.0.0.2 for HP-UX 10.10
18 April 1997

1. Scope

1.1 Identification

This Software Requirements Specification Document provides system administrators specific guidance to support COE system and software installation and maintenance.

1.2 System Overview

This version of Courtney monitors the network and identifies the source machines of SATAN probes/attacks. Courtney receives input from tcpdump counting the number of new services a machine originates within a certain window. If one machine connects to numerous services within that time window, Courtney identifies that machine as a potential SATAN host.

System configuration variables and command line options can be found in Appendix A.

2. Referenced Documents

Installation Procedures (IP) for Courtney version 1.0.0.2, 18 April 1997

3. Operating Guidelines

The default behavior of this software is to run in the background of your system without Adumping@ information to the screen.

The configuration variables and command line options can be found in Appendix A.

For the configuration variables, make changes within the /h/COE/Comp/COURT/bin/courtney.pl file. The command line options must be added at the root prompt like the example below:

None.

6. Error Recovery Guidelines

To shutdown courtney.pl, type ps -ef at the root prompt to list all of the current processes. Locate the courtney.pl process and its process number. Once you have located that number, execute the following:

```
# kill -9 <process number>
```

This will immediate kill the courtney.pl process. To restart courtney.pl, execute the following at the root prompt:

```
# /h/COE/Comp/COURT/bin/courtney.pl &
```

If courtney will not start, make sure that the first line in the courtney.pl file is calling the correct perl script. It should read:

```
#!/usr/local/lib/perl
```

If that is not correct, you need to make the correction.

Please note that there are other command line options that can be chosen instead of A&@ in Appendix A.

Appendix A. Courtney REAME file.

Name: Courtney

Date: 4/07/95
Version: 1.3

Description:

Monitors the network and identifies the source machines of SATAN probes/attacks. Courtney receives input from tcpdump counting the number of new services a machine originates within a certain time window. If one machine connects to numerous services within that time window, Courtney identifies that machine as a potential SATAN host.

Requirements:

Courtney requires that Perl v.5 be installed. It is available via anonymous FTP at the following site:

perl5 ftp.uu.net:/systems/gnu/perl5.001.tar.gz

Courtney configuration variables:

$UPDATE_INTERVAL
Specifies the time, in minutes, to update the host information.
$OLD_AGE
When updating host information, gets rid of host entries that
have timestamps older that OLD_AGE.
$HIGH_THRESHOLD
What number of services a single system must achieve before it
is considered the source of a HEAVY_ATTACK
$LOW_THRESHOLD
What number of services a single system must achieve before it
is considered the source of a NORMAL ATTACK

Turn syslog logging off. Default is to output alerts
to syslog via logger.

[-s]

Turn screen output on. Prints the same information that
is sent to syslog is also printed on the screen.

[-c]

Show the hostname that has initiated connections. This
option is good for watching the network. Does not require
the -s option.

[-m <address>]

Enables email and mails alerts to user@host. The subject
line contains the same information that syslog records.

[-h]

Print command line options.

Design:

Courtney is based on the fingerprint of any scanner, including SATAN. Scanners probe every port, or at least the more common ports, attempting to gather information about what services the target machine offers. If one machine connects to numerous services services within a brief time period, then that machine may be doing some sort of scanning.

Limitations:

Since courtney's input is from tcpdump, the filter for tcpdump must coincide with Courtney. There are 30 services that are being monitored, if you wish to remove or add one, you must make changes to Courtney=s perl script where the tcpdump filter lines are located.

When monitoring busy networks or monitoring on a slower system, some network traffic may be missed by the kernel. This has the potential to cause Courtney to fail to detect some attacks.

tcpdump and the logger program must be in the ENV{'PATH'} listing at the top of the courtney.pl script for this script to operate properly.